REMARKS -- General

A. Specification

The specification has been rewritten in light of the Examiner's rejection of certain sentences and phrases in the preliminary amendment as constituting new matter. The Applicant has decided not to contest the Examiner's determinations, without admission.

The rewritten portions 1. reinstate changes that were made without objection prior to the most recent version of the Second Substitute Specification but which had been inadvertently omitted from it, 2. reinstate phrases that had been deleted in connection with the formulation of the sentences and phrases of the Second Substitute Specification that the Examiner found objectionable, and 3. provide further explanation that may be needed for comprehension upon deletion of the objected-to matter.

The Applicant respectfully draws the Examiner's attention to the Examiner's earlier comments and instructions contained the OA of June 28, 2000, at paragraph 8, which has been followed as a guide in the rewriting process. The Examiner stated at that time:

> Claims 1-8 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Part (d) of the first claim talks about differentiating between template and boilerplate information; this information has not been mentioned in the specification. Add a brief discussion of how this step is done and what types of information constitute template and boilerplate information.
>
> Applicant says that information is "wrapped" but does not say what wrapping entails. In the examiner's experience, wrapping generally includes encryption, e.g. key wrapping. ***Please add commentary on how precisely the active X (com) object wraps the digital signature.*** There is no mention in the specification about how one would sign a message without using public key cryptography. Although the examiner is aware of

certain methods, the methods that the applicant intends need to be detailed in the specification.

The amendments required in the above paragraph ***will not necessitate filing a continuation-in-part application (CIP)*** because the first simply requires putting material that was *originally* in the claims into the specification. The second change explains more clearly a process already in the disclosure. Addition of material to the claims that is not now in the specification would require the filing of a CIP (bold and italics added for emphasis; italics only in the original).

B. Novelty

Applicant has emphasized the novelty of the invention by now requiring expressly in all independent claims that a server computer signs ***for others*** (as opposed to signing for itself), even though it does so with a single asymmetric encryption private key that is digitally certified as belonging to itself. The "others" on whose behalf it signs can include entities or individuals, or computerized agents. The invention addresses a new legal requirement of many U.S. state laws, which postulate that to be considered secure and presumptively valid as binding, an electronic signature must be unique to the signer. Thus, Arizona Revised Statutes § 41-132 provides:

> "B. an electronic signature shall be *unique to the person using it*, shall be capable of reliable verification and shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated." (Emphasis added)

See also Section 10-110 of the Illinois Electronic Commerce Security Act (1997), amended 1999, http://www.legis.state.il.us/legislation/ilcs/ch5/ch5act175articles/ch5act175sub3.htm http://www.bmck.com/ecommerce/cecc-fin.doc (report and original version).

This requirement poses a technical problem where a single private key on a server is used successively to sign by and on behalf of a plurality of signers on behalf of each of them. As between different signers, requiring that each signature be unique to a particular signer seems at first blush impossible to achieve. All signatures will be non-unique if the same private key is used for each of them.

The invention meets the legal requirement for a signature server using a single key for and on behalf of many signers by parsing unique identifying information of the signature transaction, associating it with the signer's identity and making sure that it is included under the signature as signed data, or alternatively that it is used to symmetrically encrypt the message digest or the asymmetric signature value in a second step. This teaching guarantees a relying party that the signature is unique to the signer. Since time is a river that moves in one direction only, the date and time of each transaction generally without more provides a unique identifying characteristic for each signature transaction, unless two signatures occur at practically the same time, in which case the addition of the IP address provides a grounds of further distinction between them. The same computer at the same IP address cannot logically create two different signatures at the same instant in time. The identity of the signer is then logically associated to these parameters that uniquely identify the transaction by adding identity as an element that is digitally wrapped by the server's private encryption key. Where proof of identity is additionally required, identity can be also authenticated by a credit card authorization, which is a third party assertion by a credit card gateway that the identity of the signer has been confirmed. Other means of authentication, if required, can include a biometric, username and password or PIN, or a digital certificate for web authentication purposes, and each provides a different level of assurance as to the reliability of authentication that is sought and achieved.

The data elements that uniquely identify a signature and associate it with a signer's identity can also be represented by a GUID fashioned from the various data elements to be included as signed data, and itself can be a message digest of a concatenation of them, as described in the specification.

Such data elements, as represented by the GUID, can alternatively be used to generate a symmetric key for encrypting the returned asymmetric signature value, which is used to bind the GUID and its associated data cryptographically to the asymmetric signature value.

With either method, a signature that is unique to the signer is created, meeting the legal requirement for uniqueness of a secure electronic signature, and endowing it with presumptive legal effect, even though only a single encryption key is used for signing for and on behalf of a plurality of individuals, entities and institutions as a business service.

This feature of securely signing on behalf of others with a single asymmetric private encryption key differs from the prior art by virtue of the delegated signature functionality. Timestamping as in Haber et al concerns verifying the existence of data at a particular point in time. Timestamping prevents backdating of data to make it appear that it was created earlier than it really was. It is an anti-fraud device. There is no claim by Haber that the timestamp also can serve as a signature affixed by the timestamping service on behalf of a person or entity who submitted the data for timestamping. Signing on behalf of another for legal purposes has a different purpose. It assures relying parties that the signing party cannot disavow or repudiate an obligation, representation or assurance of good faith *intended* by affixing a legal signature. See the Federal Esign Act, 15 U.S.C. section 7006 (5), which states that "the term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person *with the intent to sign the record*." (Emphasis added)

For this reason, the specification talks in terms of data, such as the date and time value, which appears "under the signature". To those skilled in the art, the term signifies that the signature is not technically a time-stamp but rather includes within the signed data that remains inalterable without detection, the date and time, in this case, to act as a unique identifying factor of the signature, in accordance with the legal requirement for a secure electronic signature.

The limitation in the claims of signing on behalf of another also distinguishes the teaching of Kocher et al. Kocher's abstract states: "The present invention provides an apparatus and method for *confirming, timestamping and archiving* documents using telecopiers (facsimile machines)" (emphasis added). No reference is made anywhere in Kocher to securely signing documents on behalf of others as part of the purpose or function of the invention. Kocher's invention meets "a need for a timestamping system that is suitable for use with paper documents, yet provides cryptographically-assured verification, and which is accessible to users with no modification to their existing document transmission devices (e.g., facsimile machines)." Col 3., lines 22-25. Kocher does not claim to affix a binding signature on behalf of another as part of its timestamping system.

Thus in response to the Examiner's comments in the OA with regards to the section 103 rejections, beginning on page 3, and included in paragraph 9 of the OA, the Examiner is respectfully requested to consider the following with regard to objections to the specific claims that were rejected:

Although Lines 26-37 of Column 7 do disclose many identifiers of a sender entity, it is imperfect to compare the archive of Kocher with the applicant's server system and the sending entity of Kocher with the applicant's client because in Kocher, the sending entity does not engage the archive to sign a document on its behalf as an intended secure signature of the sending entity. Although it is accurate to state that Element 210 of figure 2 represents the reception of a document from a client at the archive, and to conclude that Kocher's client intends to send the document to the archive, the client in Kocher does not charge the archive with the additional task of signing the data for or on behalf of the client using the private encryption key of the archive such that a party can rely upon the signature to securely bind the client to an obligation, transaction, undertaking, contract or representation of fact. The same observations apply to Element 220 of figure 2; Element 230's timestamping of the document, and the signing of the identifier. The TTI described in lines 48-52 of column 3 refers to unique identifiers of documents to be archived, but Kocher does not use the unique identifiers to meet a legal requirement of a unique signature of a signer, as does this invention, because Kocher does not claim an invention to generate a signature for or on behalf of another. Kocher does use network addresses to create unique identifiers for document retrieval purposes in lines 39-40 of column 7, and does mention credit card numbers in line 35 of column 7, and dedicated phone lines in line 30 of column 7, but Kocher does not logically associate such identifiers with the client's identity for the purpose of signing objects on the client's behalf, as does this invention. Kocher does reference RSA digital signatures in column 10, lines 39-46, but for the purpose of affixing a timestamp, not for the purpose of creating a unique and binding secure electronic signature for or on behalf of a client.

It also is true that Kocher remarks any algorithm can be used for the digital signature on lines 46-47 of column 13, although the context of the remark and the referenced algorithms indicate that the algorithms being reference are all asymmetric, and do not include a symmetric cipher, as the OA postulates. It is also true that MAC's use symmetric keys, but they are unable to be used for binding electronic signatures, as previous selections from Baum and Ford have pointed out and as was discussed in Amendment B dated June 12, 2001, which discussion is incorporated by reference herein. The authors specifically excluded at p. 320 the use of MACs as a signature protocol suitable for purposes of non-repudiation, because both the recipient and originator shared the key, and either could have affixed the encryption. As was pointed out by the selection from Baum and Ford, the fact that either party has the means to create the signature, results in a signature that is neither under the exclusive control of a signer or is unique to the signer, such that it is not recognized or usuable as a secure electronic signature under the digital signature laws previously referenced.

> However, a MAC cannot provide non-repudiation of the origin of a message because it is not adequate *to convince a third party* as to who originated the message – since two parties possessed the key, either one could equally well have originated the message." (Emphasis original)

The quoted selection from Baum and Ford underscores the difference between this invention and Kocher because this invention *is* directed "to convincing a third party as to who originated the message," while Kocher is not. Kocher does not claim non-repudiation of message origination, while this invention does by creating a presumptively valid electronic signature that meets the "uniqueness" requirement of applicable state laws for secure electronic signatures.

In none of the descriptions or claims of Kocher is there any suggestion that the archive will sign a document securely for or on behalf of a client, and the teaching of Kocher is not suggestive of the claims of this invention now that they are limited by the language to "sign for or on behalf of another".

Baum and Ford in the disclosed extract do describe a method for the affixing of a digital signature on behalf of another through a common, shared server's key, but they do not describe a method for the creation of a unique signature of the signer, making the teaching unsuitable for legal recognition as a "secure electronic signature" under applicable state laws because there is no feature that uniquely distinguishes the signatures of the various signers from each other as is described in this invention.

C. Claim Amendments

The claims include the previously presented claims 76, 77, and 78, which the Examiner indicated during the consideration of Amendment E were objectionable as new matter. Claim 76 has also been amended to include the "by or on behalf of another" limitation now applicable to all the independent claims.

Claims 99-115 are new claims that are all based upon the independent claim 99. It claims:

> An electronic signature method whereby, upon a remote command of a signer, a server uses an encryption key to digitally sign text, a binary object, or a combination of form input and a document template, and by means of a signer identifier, a date and time parameter, an IP network address, or combination of any of them, or a GUID, creates a unique electronic signature for or on behalf of the signer.

This claim encapsulates the limitations of the invention: a remote signer, a digital signature of a server, data to fashion a unique transaction ID and associate the signer with it, and a server that signs on behalf of the signer.

Claims 116-126 are also treated as new claims. This treatment was arrived at because former claim 83 was so extensively reworked that new claim 116 resulted. It could no longer legitimately be considered as simply an amendment of claim 83. The dependent claims 117-126 are similar to or identical to the claims that were dependent upon old claim 83, but it was felt that treating them as having been previously presented or amended would have placed them chronologically before the new claim 116 upon which they depended, which would have created confusion for the reader. For sake of clarity and consistency, they also have been presented as new claims.

D. Conclusion

With the limitations of securely signing "on behalf of another" in the independent claims and of means to create a unique signature of an individual signer notwithstanding a server's shared key, the learning of prior art is distinguished as inapplicable. For all of the above reasons, applicant submits that the specification and claims are now in proper form, and that the claims all define patentability over the prior art. Therefore, applicant submits that this application is now in condition for allowance, which action is respectfully solicited.

Conditional Request for Constructive Assistance

If, for any reason this application is not believed to be in full condition for allowance, applicant respectfully requests the constructive assistance and suggestions of the Examiner pursuant to M.P.E.P. Sections 706.03(d) and 707.07(j). Alternatively, if the examiner agrees that patentable subject matter is presented but does not feel that the present claims are technically adequate, applicant respectfully requests the examiner to write acceptable claims pursuant to MPEP 707.07(j).

Respectfully,

John H. Messing
Applicant Pro Se

3900 E. Broadway Blvd., Suite 201, Tucson, AZ 85711 (new address)
Tel.: (520) 547-7933 Fax: (520) 547-7920

Certificate of mailing: I certify that on the date below this document and referenced documents and attachments will be deposited with the U.S. Postal Service as first class mail in an envelope addressed to: "Mail Stop Non-Fee Amendment, COMMISSIONER FOR PATENTS, BOX 1450, Alexandria, Virginia 22313-1450."

November 26, 2003

John H. Messing
Applicant